UNDER SEAL

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
IN THE MATTER OF THE SEARCH OF 14 ELECTRONIC DEVICES DESCRIBED IN ATTACHMENT A AND LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION AT 9325 DISCOVERY BOULEVARD, MANASSAS, VIRGINIA 20109

Case No. 1:17-SW-619

Filed Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A (incorporated by reference)

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1030(a)(2)	Accessing a Computer and Obtaining Information
18 USC 1030(a)(4)	Accessing a Computer to Defraud and Obtain Value
18 USC 1030(a)(5)	Damaging a Computer or Information

The application is based on these facts:

See Attached Affidavit (incorporated by reference)

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Matthew Miller, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: Sept. 26, 2017

/s/ JFA
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

The Honorable John F. Anderson
Printed name and title

ATTACHMENT A

The property to be searched are the following electronic devices (hereinafter, "THE DEVICES"):

1) Samsung Micro SD Card from Samsung SM-G935A Cellular Telephone

2) Dell Server (ID # J3KLCY1; PowerEdge R620);

3) Corsair Homemade Tower (unknown model and serial number);

4) Seagate External Hard Drive (Model: SRD0SD0; Serial: NA5K24FC);

5) SanDisk 8GB USB Thumb Drive (black and red in color);

6) SanDisk Adapter containing SanDisk Ultra 64GB Micro SD;

7) SanDisk 32GB Thumb Drive (Serial Number: BM1504246878);

8) SanDisk Ultra 16GB Thumb Drive (Serial Number: BL130423491B);

9) Seagate Savvio 10k.2 Laptop Hard Drive (146 GB; Serial: 3NM71HBA);

10) Seagate Savvio, 10k.2 Laptop Hard Drive (146 GB; Serial: 3NM6Y0Z9);

11) Seagate Barracuda Laptop Hard Drive (1 TB; Serial: ZDE00V5P);

12) Dell Inspiron Laptop (Serial: 9YQSB62);

13) MacBook Laptop (Model: A1369; Serial: C02F21UYDJDK); and

14) Nexus Tablet (unknown serial number and black in color).

THE DEVICES are currently located at the Federal Bureau of Investigation, 9325 Discovery Boulevard, Manassas, Virginia 20109.

This warrant authorizes the forensic examination of THE DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on THE DEVICES described in Attachment A that relate to violations of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2), (a)(4), or (a)(5), and involve MARTIN MEHRAN TAHERI since November 21, 2016, including:

a. All documents, communications or other information related to the gathering or use of identities or login credentials to access VICTIM COMPANY 1's computer infrastructure, including usernames, passwords, and records of Internet activity (such as Internet Protocol ("IP") addresses, browser history, caches, cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses).

b. All documents, communications, or other information related to the unauthorized possession, transfer, or use of VICTIM COMPANY 1's confidential or proprietary information;

c. All documents, communications or other information related to end-user computer activities on VICTIM COMPANY 1's computer infrastructure, including any data collected, downloaded, or viewed by the user.

d. All documents, communications or other information related to security authentication certificates, such as secure sockets layer certificates ("SSL certificates"), pertaining to VICTIM COMPANY 1.

e. All documents, communications, or other information indicating how and when VICTIM COMPANY 1's computer infrastructure was accessed or used in order to determine the chronological and geographic context of such access or use as it relates to the crimes under investigation and TAHERI.

f. All documents, communications, or other information pertaining to the means and source of payment for services (including any credit card or bank account number or digital

money transfer account information) that were used in or otherwise relate to the crimes under investigation.

g. All documents, communications, or other information indicating TAHERI's state of mind as it relates to the crimes under investigation.

h. Passwords and encryption keys, and other access information that may be necessary to access THE DEVICES.

2. Evidence of user attribution showing who used or owned THE DEVICES at the time the things and activities described in this warrant were conducted, created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol ("IP") addresses 173.79.129.171 and 71.127.46.97 to connect with or access (or attempt to connect with or access) VICTIM COMPANY 1's computer infrastructure (to include computer servers operated or controlled by third-party vendors associated with VICTIM COMPANY 1), including:

a. records of IP addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF 14 ELECTRONIC DEVICES DESCRIBED IN ATTACHMENT A AND LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION AT 9325 DISCOVERY BOULEVARD, MANASSAS, VIRGINIA 20109	Case No. 1:17-SW-619 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE 14 ELECTRONIC DEVICES

I, Michael B. Miller, a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of 14 electronic devices that currently are in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the FBI and have been so employed since May 2016. Prior to my FBI service, I served as a state law enforcement investigator in Florida from approximately 2007 to 2016 and primarily investigated computer-related crimes. At the FBI, I am currently assigned to investigate computer-related crimes. As such, I have participated in numerous investigations involving computer and high-technology-related crimes, including computer intrusions, Internet fraud, credit card fraud, and bank fraud. Through my FBI employment, I have received training in general law enforcement and in such specialized areas

as computer and white-collar crimes. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusions and other financial crimes stated under federal law, including 18 U.S.C § 1030(a) (Computer Fraud and Abuse Act).

3. The facts and information contained in this Affidavit are based upon my training and experience, participation in this and other investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other special agents, police officers, and individuals involved in this investigation. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by review of the records, documents, and other physical evidence obtained during the course of the investigation. This Affidavit contains only the information necessary to support probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched are 14 electronic devices (hereinafter, "**THE DEVICES**") currently located at Federal Bureau of Investigation, which is at 9325 Discovery Boulevard, Manassas, Virginia 20109, within the Eastern District of Virginia. The Loudoun County Sheriff's Office seized **THE DEVICES** on or about August 4, 2017. As identified in Attachment A, **THE DEVICES** are as follows:

a. Samsung Micro SD Card from Samsung SM-G935A Cellular Telephone;

b. Dell Server (ID No. J3KLCY1; PowerEdge R620);

c. Corsair Homemade Tower (unknown model and serial number);

d. Seagate External Hard Drive (Model: SRD0SD0; Serial: NA5K24FC);

e. SanDisk 8GB USB Thumb Drive (black and red in color);

f. SanDisk Adapter containing SanDisk Ultra 64GB Micro SD Card;

g. SanDisk 32GB Thumb Drive (Serial: BM1504246878);

h. SanDisk Ultra 16GB Thumb Drive (Serial: BL130423491B);

i. Seagate Savvio 10k.2 Laptop Hard Drive (146 GB; Serial: 3NM71HBA);

j. Seagate Savvio, 10k.2 Laptop Hard Drive (146 GB; Serial: 3NM6Y0Z9);

k. Seagate Barracuda Laptop Hard Drive (1 TB; Serial: ZDE00V5P);

l. Dell Inspiron Laptop (Serial: 9YQSB62);

m. MacBook Laptop (Model: A1369; Serial: C02F21UYDJDK); and

n. Nexus Tablet (unknown serial number and black in color).

5. This Affidavit is submitted for the limited purpose of showing probable cause to believe that **THE DEVICES** contain evidence, fruits, and were themselves instrumentalities of the offenses described in Attachment B, particularly violations of 18 U.S.C. §§ 1030(a)(2), (a)(4), (a)(5) (Computer Fraud and Abuse Act). In addition, the applied-for warrant would authorize the forensic examination of **THE DEVICES** for the purpose of identifying electronically stored data that also is particularly described in Attachment B.

RELEVANT STATUTES

6. Based on my training and experience, and discussions with federal prosecutors assigned to this investigation, I have learned that 18 U.S.C. § 1030(a)(2) makes it a crime to intentionally access a computer without authorization or exceed authorized access, and thereby obtain information from a protected computer; 18 U.S.C. § 1030(a)(4) makes it a crime to knowingly and with intent to defraud access a protected computer without or in excess of authorization, and by means of such conduct further the intended fraud and obtain anything of value (including use of the computer if the value exceeded $5,000 in any year period); 18 U.S.C.

§ 1030(a)(5)(A) makes it a federal crime to knowingly cause the transmission of a program, information, code, or command, and, as a result of such conduct, intentionally cause damage to a protected computer without authorization; 18 U.S.C. § 1030(a)(5)(B) makes it a federal crime to intentionally access a protected computer without authorization and, as a result of such conduct, recklessly cause damage; and 18 U.S.C. § 1030(a)(5)(C) makes it a federal crime to intentionally access a protected computer without authorization and, as a result of such conduct, cause damage and loss.

7. Based on my training and experience, and discussions with federal prosecutors assigned to this investigation, I have learned that the term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information," the term "loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service," and the term "protected computer" includes computers "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

RELEVANT TECHNICAL TERMS

8. I have received training from the FBI related to computer systems and the use of computers during criminal investigations. Based on my education, training and experience, and information provided to me by other law enforcement agents, I know the following:

a. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries.

b. An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is typically a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. The term "computer," as used herein, is defined in 18 U.S.C. § 1030(e)(1) and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. A computer user accesses the Internet through a computer network or an Internet Service Provider, or ISP.

d. A "server" is a computer on a network that manages network resources. Authorized users on the network can store files on the server.

e. Electronic mail, or "email," is a popular method of sending messages and files between computer users. When a computer user sends an email, it is created on the sender's computer, transmitted to the mail server of the sender's email service providers, then transmitted to the mail server of the recipient's email service

provider, and eventually transmitted to the recipient's computer. Copies of emails are usually maintained on the recipient's email server, and in some cases are maintained on the sender's email server.

f. A mail or email server is a computer on a network that works as a virtual post office, *i.e.*, it stores and moves email over the network and into the Internet. When a computer user sends an email, it is created on the sender's computer, transmitted to the email server of the sender's email service providers, then transmitted to the email server of the recipient's email service provider, and eventually transmitted to the recipient's computer. An email server usually consists of a storage area where email is stored for local users, a set of definable rules which determine how the mail server should react to the destination of a specific message, a database of user accounts that the mail server recognizes and will deal with (or "serve") locally, and communications modules which are the components that actually handle the transfer of the email message to and from other mail servers and email users.

g. A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, DVDs, flash memory, CD-ROMs, servers and several other types of magnetic or optical media not listed here.

h. The term "computer systems," as used herein, means any computer, computer server, or storage medium for computer data.

i. The term "user agent string" refers to data a device provides when accessing a website or other network interface. The information in a user agent string

typically includes browser version, compatibility information, and operating system of the device.

j. The term "virtual private network," or "VPN," refers to a network that has been established to allow users to externally access an internal network securely. The data transmitted through a virtual private network typically is encrypted and secured through additional data confidentiality and integrity methods.

k. The term "secure sockets layer certificate," or "SSL certificate," refers to a cryptographic key which allows a computer user to authenticate their identity, thus enabling access to otherwise restricted areas of a computer system.

l. The term "micro SD card" refers to a miniature secure digital card that serves as a storage mechanism for digital files. These cards are found in a variety of media devices and are a standard component of many modern cellular telephones.

m. The term "backup database" refers to a copy of existing data residing within a server or other storage medium. A "backup database" is typically maintained in the event the original source of the data becomes compromised or otherwise unavailable.

n. The term "megabyte" refers to a unit of computer memory or data storage capacity.

PROBABLE CAUSE

9. The FBI currently is investigating computer- and network-related criminal activity in violation of 18 U.S.C. § 1030(a) relating to multiple unauthorized accesses of VICTIM COMPANY 1's computer network, including the unauthorized access of VICTIM COMPANY 1's servers located in Ashburn, Virginia.

10. I have learned through the course of the investigation that VICTIM COMPANY 1 provides mobile data analytics and is headquartered in Reston, Virginia. In addition, I have learned from VICTIM COMPANY 1 that it maintains computer servers in or around Reston, Virginia; Ashburn, Virginia; Milan, Italy; and Hyderabad, India. I know from my training and experience that both Ashburn, Virginia, and Reston, Virginia, are within the Eastern District of Virginia.

11. As described below, probable cause exists to believe that MARTIN MEHRAN TAHERI, a former employee of VICTIM COMPANY 1, is responsible for the unauthorized accesses of VICTIM COMPANY 1's computer network.

A. TAHERI's Employment at VICTIM COMPANY 1

12. According to VICTIM COMPANY 1, on or about January 29, 2015, TAHERI began working at VICTIM COMPANY 1 as a system administrator. TAHERI's duties as a system administrator required him to have in-depth knowledge of VICTIM COMPANY 1's computer networks, VPNs, SSL certificates, and other internal computer systems.

13. Records obtained from VICTIM COMPANY 1 indicate that, on or about November 21, 2016, TAHERI was terminated. VICTIM COMPANY 1 issued a termination letter to TAHERI the same day. The termination letter stated, in relevant part, that TAHERI's "access to [VICTIM COMPANY 1's] information systems has been removed including but not limited to: email, source code repositories, VPN, SSH, FTP, Google Apps, [and] social media service." The letter also stated: "In cases where [VICTIM COMPANY 1]'s confidential information is stored on your personal computer(s), that information must be removed as soon as possible." TAHERI signed and dated the termination letter to acknowledge he received it on or about November 21, 2016.

14. Additional records obtained from VICTIM COMPANY 1 indicate that TAHERI contacted VICTIM COMPANY 1's chief operating officer and other VICTIM COMPANY 1 staff via email on or about February 6, 2017. The email, which was sent from M3HRAN@GMAIL.COM, concerned a dispute regarding TAHERI's stock options in VICTIM COMPANY 1. TAHERI wrote, in relevant part: "I poured my heart out working long hours during my personal time even during the weekends, with even personal injury at the datacenter with pictures (bloody pictures) to prove it. Having built the infrastructure that now is up for multiple patents (without being mentioned in them) and possibly even putting you in a better position to be acquired (increased value). Is this how you show appreciation?"

B. The January 2017 Unauthorized Access

15. Records obtained from VICTIM COMPANY 1 indicate that, on or about January 29 and 30, 2017 a user accessed VICTIM COMPANY 1's network through VICTIM COMPANY 1's VPN server located in or around Milan, Italy. VICTIM COMPANY 1 has indicated that the user gained access to the VPN through log-in credentials that information technology staff at VICTIM COMPANY 1 was unaware existed. Accordingly, this user herein will be referred to as the "unauthorized user."

16. VICTIM COMPANY 1's records indicate the unauthorized user authenticated his or her access by using a valid SSL VPN certificate. It further appears from VICTIM COMPANY 1's records that after the unauthorized user accessed the VPN server in or around Milan, Italy, the user was then able to connect to VICTIM COMPANY 1's servers located in or around Reston, Virginia.

17. Through analysis of VICTIM COMPANY 1's records, including data traffic logs, and VPN logs, it appears that IP address 71.127.46.130 was used by the unauthorized user to access VICTIM COMPANY 1's server on or about January 29 and 30, 2017.

18. VICTIM COMPANY 1's records indicate the unauthorized user accessed a backup database that resided on VICTIM COMPANY 1's server and contained company data such as employee records and proprietary business related information. It appears from VICTIM COMPANY 1's records that the unauthorized user downloaded approximately 299 megabytes of data from the backup database. (VICTIM COMPANY 1 has thus far been unable to identify which specific data files were accessed and has only been able to identify the volume of data that the unauthorized user obtained.)

19. Law enforcement learned, through public information sources, that IP address 71.127.46.130 is associated with Verizon, an internet service provider. Records obtained from Verizon indicate that, at the times VICTIM COMPANY 1's server was accessed on or about January 29 and 30, 2017, IP address 71.127.46.130 was assigned to TAHERI at a residential address located in Sterling, Virginia, which is within the Eastern District of Virginia. Verizon's records also identified the email address associated with TAHERI's account as M3HRAN@GMAIL.COM.

20. This incident was unknown to VICTIM COMPANY 1 until it began an investigation concerning unauthorized access into their server subsequent to the July 2017 unauthorized access discussed below.

C. The July 2017 Unauthorized Access

21. Records obtained from VICTIM COMPANY 1 indicate that, on or about July 29, 2017, at or about 11:27 PM Eastern Standard Time ("EST"), and on or about July 30, 2017, at or

about 2:46 AM EST, an unauthorized user accessed VICTIM COMPANY 1's network through VICTIM COMPANY 1's VPN server located in or around Milan, Italy.

22. VICTIM COMPANY 1's records indicate that the unauthorized user authenticated his or her access by using a valid SSL VPN certificate. It further appears from VICTIM COMPANY 1's records that after the unauthorized user accessed the VPN server in or around Milan, Italy, the user then was able to connect to VICTIM COMPANY 1's servers located in or around Ashburn, Virginia.

23. Through analysis of VICTIM COMPANY 1's records, including firewall logs, VPN logs, and power distribution unit ("PDU") logs, it appears that IP addresses 173.79.129.171 and 71.127.46.97 were used by the unauthorized user to access VICTIM COMPANY 1's network.

24. Because VICTIM COMPANY 1's VPN servers logged the activity as it occurred, user agent strings were captured. A review of these strings indicates that IP address 173.79.129.171 was associated with a Samsung SM-G935A cellular telephone running a Linux operating system on an Android 7.0 platform and a device running a Windows operating system. Based on my training and experience, the user agent strings indicating access by two operating systems makes it reasonable to conclude that the unauthorized user utilized two different devices to access VICTIM COMPANY 1's VPN servers.

25. VICTIM COMPANY 1's records also indicate that the unauthorized user, upon connecting to VICTIM COMPANY 1's server in Ashburn, Virginia, used valid login credentials to access the server's PDU and power off 24 ports. This action resulted in an immediate loss of computer connectivity for the company and, according to VICTIM COMPANY 1, caused a disruption in service to approximately 300 of VICTIM COMPANY 1's customers. VICTIM

COMPANY 1 has reported that, as a result of subsequent remediation to this incident, VICTIM COMPANY 1 suffered a financial loss of at least $30,000.

D. Loudoun County's Search of TAHERI's Residence

26. On or about July 30, 2017, VICTIM COMPANY 1 reported the aforementioned incident to the Loudoun County Sheriff's Office in Virginia. The investigation was assigned to Detective Jason Totaro.

27. Law enforcement learned, through public information sources, that IP addresses 173.79.129.171 and 71.127.46.97 are associated with Verizon, an internet service provider.

28. On or about August 3, 2017 Det. Totaro obtained a search warrant, issued under the authority of the Commonwealth of Virginia, to obtain subscriber information for IP address 173.79.129.171 from Verizon. It should be noted that the search warrant also sought subscriber information for IP address 71.127.46.97, but it appears an error was made concerning the time and date combination listed on the warrant. As a result, the information Verizon initially returned pertaining to that specific IP address appears to relate to a customer other than TAHERI, which, based on my training and experience, likely is a consequence of Verizon assigning dynamic IP addresses to its customers.

29. Additional records obtained from Verizon indicate that, at the time VICTIM COMPANY 1's server was accessed on July 29 and 30, 2017, IP addresses 173.79.129.171 and 71.127.46.97 were assigned to TAHERI at a residential address located in Sterling, Virginia, which is within the Eastern District of Virginia.

30. On or about August 4, 2017, Det. Totaro obtained a search warrant, issued under the authority of the Commonwealth of Virginia, to search TAHERI's residence for electronic devices.

31. Just prior to executing the aforementioned search warrant on TAHERI's residence, law enforcement officers with the Loudoun County Sherriff's Office observed TAHERI leave his residence in a motor vehicle. Law enforcement officers with the Loudoun County Sherriff's Office then conducted a traffic stop on the vehicle for a traffic violation. TAHERI had a cellular telephone, a Samsung SM-G935A cellular telephone (IMEI: 352330081083300), on or about his person when he was stopped. Additionally, law enforcement later seized a Samsung micro SD card, which was inserted inside of the cellular telephone (after obtaining a search warrant, as discussed below). Law enforcement officers collected the Samsung cellular telephone from TAHERI pending the issuance of legal process. The Samsung micro SD card that was inserted inside the cellular telephone is listed as Item 1 in Paragraph 4 and Attachment A.

32. Items 2 through 14 listed in Paragraph 4 and Attachment A were collected from TAHERI's residence on or about August 4, 2017, by members of the Loudoun County Sheriff's Office pursuant to the aforementioned residential search warrant.

33. Later on or about August 4, 2017, Det. Totaro obtained a search warrant, issued under the authority of the Commonwealth of Virginia, to search the Samsung cellular telephone collected from TAHERI's person during the traffic stop. Det. Totaro reports that a member of the Loudoun County Sheriff's Office subsequently used a forensic tool to extract data from the Samsung cellular telephone. The cellular telephone was later returned to TAHERI after data was forensically extracted from the cellular telephone. The Samsung micro SD card that was inserted inside of the cellular telephone when it was seized by the Loudoun County Sheriff's Office was not returned and has remained in possession of law enforcement for additional forensic analysis.

34. Therefore, while the FBI might already have all necessary authority to examine **THE DEVICES**, I seek this additional warrant out of an abundance of caution to be certain that an examination of **THE DEVICES** will comply with the Fourth Amendment and other applicable laws.

35. On or about September 12, 2017, Detective Totaro transferred custody of all items listed in Attachment A to the Federal Bureau of Investigation. All items listed in Attachment A currently are in the custody of the Federal Bureau of Investigation, which is located at 9325 Discovery Boulevard, Manassas, Virginia 20109, within the Eastern District of Virginia. In my training and experience, I know that **THE DEVICES** have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when **THE DEVICES** first came into the possession of the Loudoun County Sherriff's Office.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

36. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. ***Wireless telephone***: A wireless telephone (or mobile telephone or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing

names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. ***Digital camera***: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. ***Portable media player***: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. ***GPS***: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. ***PDA***: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer

software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. ***Tablet***: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets typically contain programs called application, or "apps," which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

37. Based on my training, experience, and research, I know the type of information identified in the paragraph above regarding wireless telephones often is stored on the cellular telephone device itself and/or a micro SD card inserted into the cellular telephone, like the Samsung micro SD card listed as Item 1 in Paragraph 4 and Attachment A. I also know from training, experience, and research that the Nexus tablet listed in Paragraph 4 and Attachment A has several capabilities, including the ability to serve as a digital camera, portal media player, GPS navigation device, PDA, and tablet. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

38. I also know from my knowledge, training, and experience that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

39. ***Electronic Storage.*** There is probable cause to believe that things that were once stored on **THE DEVICES** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that files or remnants of files can be recovered months or even years after they have been downloaded onto an electronic device, deleted, or viewed via the Internet. Electronic files downloaded to an electronic device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the electronic device until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the electronic device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, an electronic device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic devices—in particular, devices with internal hard drives—contain electronic evidence of how an electronic device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Users

typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

40. ***Forensic Evidence.*** As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how **THE DEVICES** were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on **THE DEVICES** because:

a. Data on electronic devices can provide evidence of a file that was once on the electronic device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on electronic devices that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the electronic device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of storage devices or other external storage media, and the times the device was in use. Electronic file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on an electronic device that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the media and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device.

f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the

criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

41. ***Nature of Examination.*** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

42. Based on the foregoing, as well as the training and experience of other law enforcement personnel with whom I have spoken and my own experience, it is my belief that **THE DEVICES** contain communications and documents related that constitute evidence of the aforementioned crimes, and those items listed in Attachment B, which is incorporated herein by reference. Accordingly, I request that the Court issue the proposed search warrant authorizing the examination of **THE DEVICES** described in Attachment A, which is incorporated herein by reference.

Respectfully submitted,

Special Agent Michael B. Miller
Federal Bureau of Investigation

Subscribed and sworn to before me
on this 26th day of September, 2017

/s/ JFA
John F. Anderson
United States Magistrate Judge

The Honorable John F. Anderson
United States Magistrate Judge

Reviewed by: Alexander P. Berrang, Assistant U.S. Attorney, Eastern District of Virginia

ATTACHMENT A

The property to be searched are the following electronic devices (hereinafter, "THE DEVICES"):

1) Samsung Micro SD Card from Samsung SM-G935A Cellular Telephone

2) Dell Server (ID # J3KLCY1; PowerEdge R620);

3) Corsair Homemade Tower (unknown model and serial number);

4) Seagate External Hard Drive (Model: SRD0SD0; Serial: NA5K24FC);

5) SanDisk 8GB USB Thumb Drive (black and red in color);

6) SanDisk Adapter containing SanDisk Ultra 64GB Micro SD;

7) SanDisk 32GB Thumb Drive (Serial Number: BM1504246878);

8) SanDisk Ultra 16GB Thumb Drive (Serial Number: BL130423491B);

9) Seagate Savvio 10k.2 Laptop Hard Drive (146 GB; Serial: 3NM71HBA);

10) Seagate Savvio, 10k.2 Laptop Hard Drive (146 GB; Serial: 3NM6Y0Z9);

11) Seagate Barracuda Laptop Hard Drive (1 TB; Serial: ZDE00V5P);

12) Dell Inspiron Laptop (Serial: 9YQSB62);

13) MacBook Laptop (Model: A1369; Serial: C02F21UYDJDK); and

14) Nexus Tablet (unknown serial number and black in color).

THE DEVICES are currently located at the Federal Bureau of Investigation, 9325 Discovery Boulevard, Manassas, Virginia 20109.

This warrant authorizes the forensic examination of THE DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on THE DEVICES described in Attachment A that relate to violations of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2), (a)(4), or (a)(5), and involve MARTIN MEHRAN TAHERI since November 21, 2016, including:

a. All documents, communications or other information related to the gathering or use of identities or login credentials to access VICTIM COMPANY 1's computer infrastructure, including usernames, passwords, and records of Internet activity (such as Internet Protocol ("IP") addresses, browser history, caches, cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses).

b. All documents, communications, or other information related to the unauthorized possession, transfer, or use of VICTIM COMPANY 1's confidential or proprietary information;

c. All documents, communications or other information related to end-user computer activities on VICTIM COMPANY 1's computer infrastructure, including any data collected, downloaded, or viewed by the user.

d. All documents, communications or other information related to security authentication certificates, such as secure sockets layer certificates ("SSL certificates"), pertaining to VICTIM COMPANY 1.

e. All documents, communications, or other information indicating how and when VICTIM COMPANY 1's computer infrastructure was accessed or used in order to determine the chronological and geographic context of such access or use as it relates to the crimes under investigation and TAHERI.

f. All documents, communications, or other information pertaining to the means and source of payment for services (including any credit card or bank account number or digital

money transfer account information) that were used in or otherwise relate to the crimes under investigation.

g. All documents, communications, or other information indicating TAHERI's state of mind as it relates to the crimes under investigation.

h. Passwords and encryption keys, and other access information that may be necessary to access THE DEVICES.

2. Evidence of user attribution showing who used or owned THE DEVICES at the time the things and activities described in this warrant were conducted, created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol ("IP") addresses 173.79.129.171 and 71.127.46.97 to connect with or access (or attempt to connect with or access) VICTIM COMPANY 1's computer infrastructure (to include computer servers operated or controlled by third-party vendors associated with VICTIM COMPANY 1), including:

a. records of IP addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.